Individual Submission
INTERNET-DRAFT
Expires six months from

Vesna Hassler
Technical University of Vienna
March 1, 1998

LDAPv3 Security Parameters
<draft-hassler-ldapv3-secparam-00.txt>

1. Status of this Memo

This document is an Internet-Draft. Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To view the entire list of current Internet-Drafts, please check the "1id-abstracts.txt" listing contained in the Internet-Drafts Shadow Directories on ftp.is.co.za (Africa), ftp.nordu.net (Europe), munnari.oz.au (Pacific Rim), ds.internic.net (US East Coast), or ftp.isi.edu (US West Coast).

2. Abstract

Two security services that are required in many applications but have not been addressed by LDAPv3 [ldapv3] in a satisfactory manner yet are integrity and non-repudiation. According to the latest LDAPv3 security draft [ldapv3-auth] integrity can be achieved within a secure association only. Non-repudiation, and by this we mean digital signing of operations, is mentioned in [ldapv3] as an example of the use of the LDAPv3 extended operation mechanism.
A disadvantage of this approach is that it would be necessary to define a new Extended Request/Response pair for each basic operation that should be signed.

This document defines an LDAP control called LDAPSecurityParameters for transferring security parameters with LDAP operations.
With this control it is possible to append digital signature to LDAP operations and in this way provide for message authenticity, message integrity, non-repudiation of message origin and message freshness.

3. Table of Contents

1. Introduction

The Lightweight Directory Access Protocol (LDAP) [ldapv3] is rapidly becoming the ubiquitous mechanism for accessing and manipulating directory data. Many diverse directory implementations, data stores, client applications, and API suites are acquiring LDAP interfaces and functionality.

Two security services that are required in many applications but have not been addressed by LDAPv3 [ldapv3] in a satisfactory manner yet are integrity and non-repudiation. According to the latest LDAPv3 security draft [ldapv3-auth] integrity can be achieved within a secure association only. Non-repudiation, and by this we mean digital signature of operations, is mentioned in [ldapv3] as an example of the use of the LDAPv3 extended operation mechanism. A disadvantage of this approach is that it would be necessary to define a new Extended Request/Response pair for each basic operation

that should be signed. We propose another mechanism that requires less changes in the protocol and causes less overhead. This mechanism is based on LDAP controls which provide a general way to specify extension information. They are sent as a part of an operation and apply only to that operation. In the proposed solution we follow the X.511 security parameters concept [x511] as closely as possible.

This document defines an LDAP control called LDAPSecurityParameters for transferring security parameters with LDAP operations. With this control it is possible to append digital signature to LDAP operations and in this way provide for message authenticity, message integrity, non-repudiation of message origin and message freshness.

2. The Control

This control MAY be included in each LDAP operation as a part of the controls field of the LDAPMessage, as defined in Section 4.1.12 of [ldapv3]. The structure of the control is as follows:

```
LDAPSecurityParameters ::= SEQUENCE {
             controlType             LDAPOID -- to be assigned,
             criticality             BOOLEAN DEFAULT FALSE,
             controlValue            SecurityParameters}

SecurityParameters  :=      SET {
     certification-path      [0]     AF.CertificationPath OPTIONAL,
     name                    [1]     LDAPDN OPTIONAL,
     time                    [2]     UTCTime OPTIONAL,
     random                  [3]     BIT STRING OPTIONAL,
     target                  [4]     ProtectionRequest OPTIONAL}
     signature               [4]     AF.Signature OPTIONAL}

ProtectionRequest       :=      INTEGER { none(0), signed(1) }
```

The control type MUST be set to an OBJECT IDENTIFIER for LDAPSecurityParameters (not yet assigned). The control SHOULD be critical.

The control is specified based on the X.511 Security Parameters, which are an optional part of the X.511 Common Arguments [x511]. The use of the certification-path, name, time random and target fields are as defined in [x511] for X.511 Security Parameters.

The ASN.1 type AF.Signature (AF stands for "Authentication Framework")

is defined in [x509] as follows:

```
AF.Signature            :=      SEQUENCE {
     algorithmIdentifier     AlgorithmIdentifier,
     encrypted               BIT STRING}
```

The value of the encrypted field is computed over the entire LDAPMessage with the encrypted field set to NULL (i.e. absent). The ASN.1 type AF.CertificationPath is defined in [x509].

The algorithmIdentifier must be an entirely numeric string representation of an OBJECT IDENTIFIER.

2.1. Encoding Requirements

(This section is identical to Section 4 in [ldapv3-strong].) This document describes data elements using ASN.1 structures, which are encoded using a subset of the Basic Encoding Rules, as done in LDAPv3 [ldapv3]. Implementations must follow the encoding restrictions of LDAPv3, and additional encoding restrictions apply to the elements defined in this specification:

- BIT STRING values are to be encoded in primitive form only. Unused bits in the final octet of the encoding of a BIT STRING value, if there are any, should always be set to zero.

- UTC Times must be encoded with the "Z" suffix, not as a local time.

3. Client-Server Interaction

The control MAY be used in all LDAPv3 operations (note the difference from X.511, where it cannot be used in the bind request/response). In this section we describe some of the possible use scenarios.

3.1. Client's Signature

If the server sends the control in the bind response, with the target field set to signed(1), the client MUST sign all subsequent requests until the next unbind request. If the server does not insist on signing its own messages (i.e. responses), the certification-path field in the control MUST be absent. Note that the control is not signed and therefore can be tampered with.

With this mechanism all client requests can be
authenticated using a strong authentication mechanism,
and the signature can be for non-repudiation of message origin.
However, this mechanism alone does not provide for either
confidentiality of any data transferred between the client
and the server, or for the authenticity of the data transferred
from the server to the client.

If the server sends the control in any response message
except the bind response, with the target field set to signed(1),
the client MUST resend the request with the control carrying
the signature. The security considerations are the same as
in the previous paragraph.

If the client sends a request (i.e. any request except the bind
request) without the control carrying the signature, and the server
requires the request be signed, the server MUST return
inappropriateAuthentication as a result code, and the control with
the target field set to signed(1).

3.2. Server's Signature

If the client sends the control in the bind request,
with the target field set to signed(1), the server MUST either return
unavailableCriticalExtension as a result code,
or sign all subsequent responses until the next unbind request.
If the client does not insist on signing its own messages
(i.e. requests), the certification-path field MUST be absent.
If the server's certificate has been sent in the bind response,
it MAY be omitted in the subsequent server responses.
The server MAY set the time field of the control to
currentTime (see Section 4.). Note that the control is not signed and
therefore can be tampered with.

With this mechanism all server responses can be authenticated
using a strong authentication mechanism,
and the signature can be used for non-repudiation of message origin.
However, this mechanism alone does not provide for either
confidentiality of any data transferred between the client
and the server, or for the authenticity of the data transferred
from the client to the server.

If the client sends the control, with the target field
set to signed(1), as part of any request except the bind request, the
server MUST either return unavailableCriticalExtension as a result
code, or sign the corresponding responses.

3.3. Client's and Server's Signature

To provide for authenticity and non-repudiation (which also implies integrity) of all data transferred between the client and the server, both the client and the server MUST sign their messages. If the time and random field of the control are used in an appropriate way, the protection against reply attacks (i.e. message freshness) can be provided.

If the signed operations requestor (i.e. client or server) sends its certification-path in the control with the target field set to signed(1), both the receiver (i.e. server or client) and the requestor MUST sign the messages as defined in Sections 3.1. and 3.2. The requestor SHOULD sign the message carrying the control, otherwise the sign request can be tampered with.

4. Attributes in the Root DSE

[ldapv3-strong] defines four attributes which MAY be present in the server's root DSE:


```
currentTime - for checking the current time
serverName - for validating the name of the server
certificationPath - for obtaining the certification path from
                    the server
supportedAlgorithms - for determining the supported signature
                      algorithms
```

5. Security Considerations

This document describes a new security mechanism for LDAPv3. Security is discussed in the previous sections.

6. References

[ldapv3]
M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3), RFC 2251, http://ds.internic.net/rfc/rfc2251.txt

[ldapv3-strong]

M. Wahl, "X.500 Strong Authentication Mechanisms for
LDAPv3", INTERNET-DRAFT <draft-ietf-asid-ldapv3-strong-00.txt>,
March 1997,
ftp://ietf.org/internet-drafts/draft-ietf-asid-ldapv3-strong-00.txt

[ldapv3-auth]
M. Wahl, H. Alvestrand, "Authentication Methods for LDAP",
INTERNET-DRAFT <draft-ietf-ldapext-authmeth-01.txt>, Jan 1998,
ftp://ietf.org/internet-drafts/draft-ietf-ldapext-authmeth-01.txt

[x509]
ISO/IEC 9594-8 (ITU-T X.509), "Information technology -
Open Systems Interconnection - The Directory: Authentication
framework", 1995,
http://www.iso.ch/

[x511]
ISO/IEC 9594-3 (ITU-T X.511), "Information technology - Open Systems
Interconnection - The Directory: Abstract service definition", 1995,
http://www.iso.ch/

7. Author's Address

Vesna Hassler
Technical University of Vienna
Distributed Systems Group 184-1
Argentinierstrasse 8/3rd floor
A-1040 Vienna
Austria

Phone: +43 1 58801 4426
Fax: +43 1 5058453
Email: hassler@infosys.tuwien.ac.at